



Group Policy for the Management of the Money Laundering and Terrorism Financing related risks

Modena, 17 October 2019 – summary version

TABLE OF CONTENTS

1 MAIN TOPICS COVERED

2 SCOPE OF THE DOCUMENT

3 REGULATORY REFERENCE FRAMEWORK

4 BEHAVIOURAL GUIDELINES FOR THE BPER GROUP

5 ROLES AND RESPONSIBILITIES

1 Main topics covered

This document covers the main areas on which the anti-money laundering and counter-terrorism legislation is based, i.e.:

- customer due diligence;
- the obligations of data and information storage as well as sending aggregate data to the FIU;
- active cooperation required from the Group's banks and companies through the reporting of suspicious transactions;
- personnel training obligations.

The prohibitions and the thresholds regarding the use of cash and bearer securities are outlined as well.

With specific regard to countering the financing of terrorism, the compliance procedures in relation to the freezing of funds and related reporting obligations are reported.

The major updates to the previously applied - and simultaneously abrogated - "Group Policy for mitigating the risk of non-compliance with anti-money laundering and counter-terrorism legislation" (2015 edition), concern the update of the legislation provisions to comply with the novelties introduced by Leg. Decree 90/17 and Leg. Decree 231/07, from the Regulations published by the Bank of Italy on 26 March and 30 July 2019 respectively, "on the organisation, procedures and internal controls adopted to prevent the involvement of intermediaries for the purpose of money laundering and terrorism financing" and "on customer due diligence for countering money laundering and terrorism financing".

2 Scope of the document

The Policy lays down the guidelines applicable to the conduct, organisation, procedures and internal controls that the Group adopts to assure full compliance with primary and secondary legislation, in order to effectively react against the involvement, even unintentional, of the Banks and Companies belonging to the BPER banking Group in money laundering and terrorism financing.

3 Regulatory reference framework

- EU Directive 2015/849;
- Italian Legislative Decree No. 109 of 22 June 2007;
- Italian Legislative Decree No. 231 of 21 November 2007;
- Provisions concerning the organisation, procedures and internal controls aimed at preventing the involvement of intermediaries for the purpose of money laundering and terrorism financing, published by the Bank of Italy on 26 March 2019;
- Provisions related to customer due diligence for countering money laundering and terrorism financing, published by the Bank of Italy on 30 July 2019.

4 Behavioural guidelines for BPER Group

Risk definition

In compliance with the provisions of applicable legislation, risk of money laundering and terrorism financing (hereinafter also "money laundering risk") shall mean *"the risk arising from the violation of law provisions, of a regulatory and self-regulatory nature, aimed at preventing the use of the financial system for the following purposes: money laundering, terrorism financing or financing of programs for developing weapons of mass destruction, as well as the risk of involvement in cases of money laundering and terrorism financing or financing of programs for developing weapons of mass destruction"*.

Risk Management

The Group has adopted a risk management model based on which the risk of money laundering is assumed on a decentralised basis, but always under the coordination and guidance of the Group Parent Company. This defines the strategic guidelines for handling the risk of money laundering and the anti-money laundering controls, while the activities for risk management are performed on a centralised basis by the Group Parent Company.

The organisational solution adopted by the Group envisages identifying, within the Group Parent Company, an organizational unit entrusted with the Anti-Money Laundering Function¹, referred to as Anti-Money Laundering Department, in staff to the CEO and that operates, for the Group Companies, by means of an "Anti-Money Laundering Function Reference Officer".

The Anti-Money Laundering Function performs, in particular, direction and coordination activities - related to its mission - for all the Group Companies subject to anti-money laundering legislation and namely:

- Banking Companies of the Group with registered office in Italy (hereinafter also referred to as "Italian Banks");
- Non-banking Companies of the Group with registered office in Italy and subject to anti-money laundering and counter-terrorist obligations² (hereinafter also referred to as "Non-banking Companies");
- Banks or Companies of the Group subject to anti-money laundering and counter-terrorism obligations with registered office abroad³ (hereinafter also referred to as "Foreign Companies").

The Anti-money Laundering Department also performs a second level control function relating to anti-money laundering and counter-terrorism for the Parent Company and the Group Banks and companies based in Italy.

In order to properly perform its office, the Anti-Money Laundering Function shall:

- act independently, since it is separate from the other control functions and is detached, in terms of organisation, from the functions involved in risk assumption;
- be provided with suitable resources, in terms of quality and quantity, to perform the tasks required with regard to staff number, composition and technical professional knowledge;
- refer directly to the bodies with strategic supervisory functions and have access to all the data, information, archives, corporate assets and all the Group activities performed both at the

¹See Provisions concerning the organisation, procedures and internal controls on anti-money laundering dated 26 March 2019.

² At the date of this Policy, the Group non-banking Companies subject to anti-money laundering and counter-terrorist obligations are the following:

- Emilia Romagna Factor S.p.A. (BPER Factor);
- Sardaleasing S.p.A. (SARDAFACTORING);
- Optima S.p.A. SIM;
- BPER Trust Company S.p.A.
- Finitalia S.p.A.

³ At the date of this Policy, the Foreign Companies of the Group are BPER Bank Luxembourg S.A., with registered office in Luxembourg.

headquarters' offices as well as at the peripheral organizations; it shall also have access to any and all information that is relevant for its own tasks, and that may be also obtained by means of individual interviews with the staff.

BPER Banca, acting as Parent Company, is responsible for defining the guidelines to govern and manage the money laundering risk for the entire banking Group, and in particular for:

- assuring that the money laundering risk model, the group strategies and policies are suitably implemented, both individually within each Group company, as well as on a consolidated level;
- assuring that the money laundering risk model is drawn up in compliance with the provisions established by the Supervisory Authorities, taking into account the specific characteristics of the Group and of its individual companies;
- establishing and approving a group method for assessing the money laundering risks, in compliance with the method identified by the Supervisory Authority within the scope of money laundering risk "self-assessment" practices⁴;
- establishing and approving formalised procedures for coordinating and sharing relevant information among the Group Companies. To this end, the Parent Company issues, in particular, a shared information basis, to allow all Group Companies to homogeneously evaluate their customers⁵;
- establishing and approving general standards regarding customer due diligence, data storage and identification and reporting of suspicious transactions.

These principles are substantially implemented by adopting the management model for the risk of money laundering formalised in this Policy. This provides clear rules for assigning roles and responsibilities and for separating the functions responsible for the processes of risk assumption and risk operational management from those responsible for non-conformity risk management and control, assuring that roles and responsibilities are independent from each other.

In putting in place the guidelines established by the Parent Company, the principles of gradualness and proportionality shall also be observed, based on the specific characteristics of the different companies belonging to the Group and falling within the scope of consolidation.

Within the BPER Group, the role of the Chief Anti-Money Laundering Officer (CAMLO) - pursuant to the Provisions on organization, procedures and internal controls adopted by the Bank of Italy on 26 March 2019 - shall be assigned to the Head of the Anti-Money Laundering Department, who shall furthermore play the following roles, as indicated in the regulations:

- Head of the Anti-money Laundering Department, as reported pursuant to the Communication dated 7 June 2011 of the Bank of Italy, for all the Group Companies within the scope of consolidation and under Italian Law;
- STR (Suspicious Transactions Reports) Responsible Officer for BPER Banca pursuant to Art. 36, par. 6 of Leg. Decree 231/07;
- STR Responsible Officer for the Group Companies under Italian Law, that have delegated the role envisaged pursuant to Art. 36, paragraph 6, of Italian Leg. Decree 231/2007 (Group STR Responsible Officer);
- Group STR Responsible Officer for foreign companies without assignment of the role delegation as provided for by Art. 36, par. 6 of Leg. Decree 231/07.

Risk assumption and mitigation

In order to mitigate the risk of money laundering and terrorism financing, the Group adopts the protection measures and implements the controls and procedures identified based on the instructions received by the Supervisory and competent Authorities, i.e. as a result of the assessment activities carried out by the Anti-Money Laundering Department, in particular through:

- self-assessment of the risk of money laundering and terrorism financing, organised in compliance

⁴ Provisions issued by the Bank of Italy on the organisation, procedures and internal controls, dated 26/3/2019, Section Seven.

⁵ Sharing information with the Group Foreign Companies shall be applied subject to the limitations provided by applicable legislation in the hosting country.

with the instructions provided by the Supervisory Authority⁶ and conducted taking into account the risk factors linked to the type of customers, geographical area of the transactions, distribution channels as well as services and products offered;

- “ex ante” evaluations concerning the appropriateness of activities or processes and procedures not yet adopted, in order to represent the risk of money laundering that would be assumed if such activities/processes/procedures were performed or introduced without adopting further mitigation measures, and in order to identify proposals aimed at mitigating the same risk;
- “ex post” evaluations concerning verification of the appropriateness and/or effectiveness of the organisational measures adopted to prevent or mitigate the risk of money laundering, i.e. the risk that the event connected with failure to observe a regulatory provision occurs.

Protection measures within the scope of anti-money laundering and counter terrorism financing

The following part of the document outlines the general *standards* regarding the procedures and protection measures defined by the Parent Company for the Group, in order to assure that applicable legislation is observed in relation to the major fields of reference, and to assure that information is consistent and shared on a consolidated level.

4.1 Customer due diligence obligations

In order to comply with applicable legislation on customer due diligence, the Parent company establishes that the following protection measures be observed:

- perform the due diligence procedures applicable to customers pursuant to articles 17 and the following of Italian Leg. Decree 231/07:
 - when an ongoing relationship is established;
 - when occasional transactions are performed, as instructed by the customers, that involve transferring or moving means of payment above or equal to the threshold set by legislation⁷, regardless of whether such amounts are transferred by means of an individual transaction or several transactions that appear to be linked to each other in order to carry out a fractioned transaction;
 - when occasional transactions are performed, as instructed by the customers, that consist in transferring funds as defined by Art.3, par. 1, point 9 of (EU) Regulation No. 2015/847⁸ of the European Parliament and Council, and that exceed the threshold set by legislation⁹;
 - when the Bank acts as intermediary or takes part in a cash money or bearer security transfer, performed for any reason between different subjects, having an amount equal to or higher than the threshold set by the legislation¹⁰;
 - when there is a suspicion of money laundering or terrorism financing, regardless of any applicable derogation, exemption or threshold;
 - when there are doubts as to the truthfulness or adequacy of the information previously acquired for the purpose of identifying a customer;

⁶ Pursuant to the Provisions issued by the Bank of Italy on the organisation, procedures and internal controls, dated 26 March 2019, Section Seven.

⁷ Given the variability over time, the term “threshold set by legislation” shall be used in this Policy. On the date of entry into force of this Policy, the threshold is equal to EUR 15,000, as provided for by Italian Leg. Decree 231/07.

⁸The Regulations mentioned define as “fund transfer” a transaction made, at least partially, via electronic means on behalf of a transferor by a payment service provider, with the aim of making funds available to the beneficiary through a payment service provider, regardless of the fact that the transferor and the beneficiary are the same subject and that the transferor's payment service provider and that of the beneficiary coincide. Among these transactions we can mention: a) bank money transfer, as defined under Article 2, point 1), of (EU) Regulation no. 260/2012; b) direct debit, as defined under Article 2, point 2), of (EU) Regulation no. 260/2012; c) money remittance, both national or cross-border, as defined by Article 4, point 13), of directive 2007/64/CE; d) money transfer made using a payment card, an e-money tool or a mobile phone, or any other prepaid or post-paid digital or information device having similar characteristics.

⁹ On the date of entry into force of this Policy, the threshold is equal to EUR 1,000, as provided for by Italian Leg. Decree 231/07.

¹⁰ On the date of entry into force of this Policy, the threshold is equal to EUR 15,000, as provided for by Italian Leg. Decree 231/07.

- with regard to the customers already acquired, envisage renewal of the customer due diligence or assessment of the customer profile in the event that the risk linked to the same customer has increased, or in the event of major variations in their subjective or operational characteristics;
- identify the customers¹¹ and verify their identity based on the documents, data or information obtained by reliable and independent sources;
- identify the person who performs the transactions, if any, and the “beneficial owner” and verify their identity based on the documents, data or information obtained by reliable and independent sources;
- verify the actual existence of the power of representation, when the customer is a company or body, and acquire the necessary information to identify and verify the identity of the representatives with power of signature;
- verify any political exposure of the subjects identified (the so called “politically exposed persons”) and namely the repeated presence of their names in the list of terrorism supporters, also by consulting the specific reference “black lists”.
- acquire information on the scope and nature of ongoing relationships and transactions¹², verifying the compatibility of the data and information provided by the customer, also with regard to the overall transactions performed during the relationship with the same;
- adopt enhanced customer due diligence measures if there is high risk of money laundering or terrorism financing in order to exclude, already when first establishing contact with the customer, any potential involvement in illegal activities;
- evaluate the adoption of “simplified measures” for customer due diligence if low risk ratings are identified, as defined by art. 23 of Italian Leg. Decree 231/07;
- perform continual monitoring activities during ongoing relationships with the customers, by examining the overall transactions of the same customers, verifying and updating the data and information acquired also with regard to the origin of funds and resources available to the same customers, keeping the documents, data and information owned up to date. As concerns the customers having a higher risk-rating, the information acquired shall be updated at least every year; for customers having a moderate (medium) risk rating, the information shall be updated at least every three years;
- have third parties perform due diligence obligations in compliance with the provisions of articles 26 and the following of Italian Leg. Decree 231/07;
- refrain from establishing ongoing relationships or executing transactions, or terminating already existing ongoing relationships, if it is not possible to comply with customer due diligence obligations, considering also the opportunity to submit a report to the FIU;
- refrain from executing transactions suspected of money laundering or terrorism financing. Should it not be possible to refrain from the above, due to law obligations that provide for document reception, the obligation of immediate reporting of the suspicious transaction shall apply.

4.2 Obligations of customer risk profiling

In order to assure full compliance with applicable legislation on the assessment obligations of customer-related money laundering risk and risk profiling, the Parent Company establishes, for the Group, the following behavioural and organisational guidelines:

- identify the money laundering “risk profile” of the customers and assure this is regularly updated, also in order to apply differentiated customer due diligence processes based on the risk linked to the same customers;
- to this end, adopt processing systems defined by the Parent company (or however shared with the

¹¹ The identification procedure shall be carried out in the presence of the customer or, if this is not a private individual, of the person who performs transactions, subject to cases of “non-face-to-face transactions”, if any.

¹² In particular, information regarding the following shall be acquired and evaluated: the purpose of the relationship; the relationships between the customer and the person who performs the transactions and between the customer and the beneficial owner; the business and economic activity performed and, in general, the business relationships of the customer. The information may be requested to the customer or gathered from the report.

same), based on the assessment criteria and on the risk factors defined by national reference legislation and by the provisions established by the Supervisory Authority and weighed based on their relative importance;

- adopt, for the same customer, the highest risk profile among those assigned by all the Group Companies (the so called "Group risk profile"), requesting the Parent Company - based on clear written motivations - to provide express authorisation if a lower risk profile is considered more appropriate than that assigned by the other Group companies;
- periodically assess the customer risk profile and, in addition to pre-established deadlines, such risk profile shall be assessed based on any higher risk rating attributed to the customer by the corporate Procedures, applicable when events or circumstances that may change the risk profile occur (e.g. when a person is identified as PEP, in the case of major changes in the customers' activity or in their corporate shareholding).

4.3 Enhanced due diligence obligations

In order to assure full compliance with applicable legislation regarding customer due diligence, the Parent Company establishes for the Group, in addition to the provisions outlined above, the following behavioural and organizational guidelines:

- adopt "enhanced measures" for customer due diligence in the event of a high risk of money laundering and terrorism financing. To this end, the risk factors laid down by Art. 24 of Italian Leg. Decree 231/07¹³ shall be taken into account. These refer to the customer (residency in high-risk geographical areas, business activities characterised by high use of cash money etc.), to products, services or transactions (products that may help anonymity, payments received by third parties without a clear connection organisation with the customers or their business activities etc.) or are linked to geographical factors (high risk third countries);
 - the following shall always be rated as high-risk:
 - ongoing relationships or occasional transactions with customers and their related beneficial owners, that are identified as politically exposed persons;
 - cross-border relationships with a correspondent banking or financial intermediary based in a third country.
 - customers residing in high-risk rated third countries, or transactions with the same countries;
 - customers who perform transactions characterised by unusually high amounts, or transactions that may generate doubts regarding the purposes for which they are actually pre-ordered;
 - customers who are assigned a "high" money laundering risk profile based on internal calculation procedures, or for which a high risk is perceived;
 - customers whose names are listed in the so called national and international terrorism "black-lists";
 - the relationships established with organisations that may be identified as means of asset mediation, such as trust and fiduciary companies, i.e. companies incorporated or capitalised via bearer shares or with shares owned by trustees;
 - the transactions connected with public tenders and financing
 - the relationships established with non-profit organisations
 - special transactions in cash or bearer securities, such as: cross-border movement of cash and bearer securities, use of high denomination banknotes, frequent and unjustified transactions;
 - perform in-depth analyses regarding, amongst other things, the following cases potentially exposed to higher risk of involvement in money laundering:
-

- repeated application, in relation to the customer, the beneficial owner or the person who performs the transactions, of negative reputation rating (connected with crime proceedings, damage to the tax authorities or administration responsibilities; repeated application of administrative fines due to violations of anti-money laundering provisions; existence of previous reporting of suspicious transactions sent to the Financial Intelligence Unit (FIU) or of negative news from public information sources), performing the following:
 - (i) further analyse the content of the said negative information, contacting the competent corporate departments or conducting further investigations on public sources, also in order to evaluate the opportunity to refrain from continuing current relationships;
 - (ii) carry out more frequent and in-depth inspections on the transactions put in place by the customer, in order to promptly detect any anomalous/suspicious elements;
 - (iii) keep up-to-date the information regarding the origin of funds used for current relationships, as well as the economic and equity/asset situation of the subject concerned (acquiring, by way of example, financial statements, VAT and income statement returns, documents issued by the employer or other intermediaries);
- business activities characterised by high use of cash money - such as, by way of example, cash-for-gold, money exchange, gaming and betting, money remittance sectors - by means of the following:
 - (i) verification - by access to the public registers - of the existence of the required authorizations/licenses;
 - (ii) acquisition of the information required to determine the expected movement of cash, in order to identify deviations that may originate suspicious elements;
- business activities linked to sectors particularly exposed to corruptions risks such as, by way of example, in addition to those involved in the granting of public funding and tenders: health, building, weapon trading, defence, war, mining, waste collection and disposal industries, production of renewable energies - by means of the following:
 - (i) conducting an in-depth analysis of the information on the customer's proprietary and control assets, there including acquiring and evaluating information on the reputation rating of the customer and of the beneficial owner;
 - (ii) observing more careful and frequent analysis and update methods for the information available, in relation both to customer identification and to the transactions recorded;
 - (iii) keeping up-to-date the information on the origin of funds used for the account activity, as well as regarding the economic and equity situation of the subject concerned (acquiring, by way of example, financial statements, VAT and income statement returns, documents issued by the employer or other intermediaries);
- repeated listing of customers/beneficial owners that hold public roles in fields that may not be defined as "politically exposed persons", but for whom a major exposure to the risk of corruption exists, performing the following:
 - (i) acquire and keep up-to-date the information concerning the type of office or role held;
 - (ii) constantly monitor the transactions recorded during the relationship, in order to detect, in particular, unjustified cash movement or transactions that are inconsistent with the economic profile of the subject concerned;
- services with a high personalisation degree (such as asset management) provided to customers who own high asset amounts, envisaging the following:
 - (i) conducting specific in-depth analyses regarding the economic/equity/asset situation of the Customer connected with the funds,
 - (ii) in addition to analysing the consistency of the service provided with respect to the position of the same customer
 - (iii) and continually and regularly updating the acquired data;
- submit the projects concerning the adoption of new products and commercial practices - that may potentially expose the Group to money laundering/terrorism financing risks - to prior assessment of the Anti-Money Laundering Department, so that they may verify the possible risks as well as consequent and appropriate mitigation actions.

4.4 Simplified obligations of customer due diligence

In order to assure compliance with applicable legislation on customer due diligence, the Parent Company establishes the following behavioural guidelines for the Group:

- the possibility of observing simplified due diligence methods is allowed in the event of low risk factors, such as:
 - opening relationships or performing transactions on behalf of: (i) public administration offices (or institutions or bodies performing public functions in compliance with European Union law); (ii) National and EU banks; (iii) Insurance companies; (iv) Electronic money institutions that are allowed to adopt simplified due diligence methods as regards the extent of the information gathered and the data verification methods¹⁴. They are actually allowed to use a specific due diligence form more that is more simplified than the "standard" one and more delayed schedules for ordinary data update. As concerns risk profiling, a different rating may be considered for risk factors that are normally used to take into account lower risks connected with this type of customers¹⁵;
 - use of electronic money products, in the event that the conditions laid down under art. 23, par. 3, lett. a) – f), of Leg. Decree 231/07 are cumulatively observed. In this case, it shall be possible to adopt simplified due diligence methods as regards the extent of the information gathered, as well as the methods and/or timing for their collection, based on specific evaluations that shall be referred to the Anti-Money Laundering Department;
 - other low risk factors connected with: (i) type of product (e.g., products with limited functionalities, subject to specific expense limitations or characterised by ownership transparency); (ii) repeated involvement of a subject among those admitted to listing on regulated markets; (iii) geographical areas where the customer is based/the transaction refers to, for which a reduction of the information to gather¹⁶, or of the update frequency may be allowed subject to a specific assessment to be conducted from time to time. Such assessment shall be based on all the elements available, if necessary also by contacting specialised monitoring organisations;
- The possibility to observe simplified measures shall be ruled out in the event of doubts, uncertainties or inconsistencies relating to the identification data and to the information acquired upon identification of the customer, the person who performs the transactions or the beneficial owner, or whenever money laundering or terrorism financing are suspected; it is further established that, during the term of the relationship, the pre-requisites that allowed the observance of due diligence simplified measures shall be verified to check whether they persist, and it is envisaged, if such pre-requisites are no longer applicable, that ordinary due diligence methods be observed. In the same manner, ordinary verification methods shall be observed in the event that the monitoring activities on the customer's transactions, or the information acquired during the term of the relationship lead to rule out that a low risk level persists or, however, if money laundering or terrorism financing are suspected.

4.5 Non-face-to-face transactions and identification

In order to comply with reference legislation on customer due diligence, the Parent Company establishes that the following protection measures shall be observed in those cases where the identification or operational activities are identified when the customer (or the person who performs the transactions) are not physically present:

- observe the customer identification obligations by acquiring the identification data, alternatively:
 - from public documents, certified private deeds or eligible certificates used for generating digital signatures associated with information documents pursuant to Art. 24, Leg. Decree 82/2005;

- by verifying ownership of a digital identity with the greatest security level or of a certificate used for generating digital signatures pursuant to art. 19, par. 1, lett. a), of Leg. Decree 231/07;
- from a declaration issued by the Italian Diplomatic Mission or Consular authority¹⁷;
- as regards customers whose identification data have already been acquired in relation to another current and ongoing relationship, the identification obligations shall be considered observed on condition that the information held is updated and suited to the customer risk profile and to the characteristics of the new relationship;
- aside from the above mentioned cases, meet the identification obligations by verifying the ID details information declared by the customer on the copy of a valid ID document sent by fax, mail, e-mail or other similar methods and by further verifying - in addition to the *standard* verification methods pursuant to art. 4.1 - the data acquired, using methods deemed appropriate and proportionate to the risk connected with the type of customer and/or product/service, based on *ad hoc* assessments made, from time to time, by the Anti-Money Laundering Department of the Parent Company. In this regard, as a result of specific assessments conducted by this organisation service - aimed at further analysing the risk profile and minimum security requirements to adopt in relation to the possible different remote verification methods - the following shall be generally deemed an appropriate instrument, therefore usable to perform the above mentioned monitoring activities:
 - bank money transfer ordered by a customer from a current account already held by the same with a banking and financial intermediary based in Italy or in an EU country¹⁸;
 - verification of the presence of RID (direct interbank relationship) alignment or, within the scope of SEPA Direct Debit, reception of a SEDA electronic flow in acceptance of a new banking order on the account issued by the beneficiary, if routed to an account held with a banking and financial intermediary based in Italy or in an EU country¹⁹;
 - digital and remote video identification systems configured with an audio/video recording setting compliant and specifically regulated by the Bank of Italy²⁰;
 - video identity recognition through webcam by an operator responsible for remote identification with concurrent ID verification. ID must contain a picture and qualified certificate with digital signature²¹;
 - issuance of a certificate, by an Italian or EU banking or financial intermediary, that confirms proper identification of the subject person in relation to the establishment of an ongoing relationship or to the performance of an occasional transaction. Such certificate shall bear, as minimum requirement, the identification data of the subject concerned and the reference data of the ID used for the purposes of identity verification;
 - other verification methods that may be deemed appropriate by the Anti-Money Laundering Department in relation to the individual cases.

4.6 Data and information storage obligations and aggregate data transmission to the FIU

In order to comply with the reference legislation concerning data and information storage and sending of aggregate data, the Parent Company establishes that the following protection measures be observed:

- store the documents, data, information and records concerning the transactions useful to prevent, identify or ascertain possible activities of money laundering or terrorism financing, and to allow performance of the analyses conducted by the FIU or by other competent Authorities;
- specifically, keep a copy of the documents acquired upon customer due diligence and of the documents and records related to the transactions, according to the provisions of applicable national legislation (articles 31 and 32, Legislative Decree 231/07) and of the Supervisory Authority;
- adopt storage methods suitable to assure prompt and full accessibility and acquisition, integrity and inalterability, transparency, clearness and completeness, as well as historical recording of the same documents;
- store the documents, data and information acquired for a period of ten years as of the termination of the ongoing relationship or following the occasional transaction performed²²;
- notify the FIU of the aggregate data gathered in compliance with the methods established by the same (the so called S.AR.A. - Aggregate anti-money laundering reports - flows).

4.7 Personnel training obligations

In order to comply with the reference legislation concerning personnel training, the Parent Company establishes that the following protection measures be observed:

- comply with the updated guidelines on the perpetration methods of money laundering and terrorism financing crimes, as provided by the competent Authorities, in particular by the FIU, by Guardia di Finanza (Italian tax Police) and by DIA (Antimafia Investigation Directorate)
- deliver training courses differentiated by role and function, addressed to all employees and collaborators, so that they may receive appropriate knowledge of relevant legislation and related responsibilities, and so that they will be able to use the instruments and procedures adopted for proper application of the law provisions;
- define, for the persons in charge of risk protection measures at the central Departments, high-profile and suitable training, provided by external organisations;
- continually update the educational material in compliance with legislative and regulatory developments;
- monitor actual attendance of employees and collaborators to the training courses provided.

4.8 Reporting obligations for suspicious transactions

In order to comply with the reference legislation concerning reporting of suspicious transactions, the Parent company establishes that the following protection measures be observed:

- report a suspicious transaction when there is knowledge, suspicion or reasonable grounds to suspect that attempted money laundering or financing of terrorism are being carried out or have been carried out;
- assure the greatest confidentiality on the identity of the employees who report the suspicious transaction; in this regard, the interested party or third parties must not be informed that a suspicious transaction has been reported or is under way or that an inquiry regarding money laundering or financing of terrorism may be carried out;
- envisage suitable procedures for detecting potentially suspicious transactions by analysing the customers' account activity (periodic monitoring of transactions) and by identifying those transactions that are "unexpected" also based on the anomaly indicators provided by the Bank of Italy and by the

²² With regard to the Group foreign Companies, reference may be made to any other different period of time provided for by local legislation.

FIU;

- envisage procedures suitable to assure that all documentation concerning transactions which must be reported to the FIU is promptly sent to the STR Responsible Officer by the operators and managers of operational centres or organization units that handle the relationships with the customers²³;
- envisage procedures suitable to assure traceability of the reporting processes and store evidence of the evaluations expressed by the operators and by their Managers in relation to the opportunity to notify or dismiss a potentially suspicious transaction;
- envisage integrated management of corporate information coming from the Group Companies and Banks, as well as from external Companies, in relation to possible phenomena of money laundering or terrorism financing;
- periodically send, according to the methods and criteria defined by the FIU, data and information identified based on objective criteria regarding transactions featuring risks of money laundering or terrorism financing (the so called "objective communications")²⁴;
- store and keep the documentation regarding the data and information collected during the investigation phase, and assure access to such archive to internal and external entities appointed to perform inspection functions, for a period of no less than 10 years;
- promptly inform the body appointed with strategic function and the control body about the main problems that have emerged with regard to the procedures for identifying and reporting suspicious transactions;
- appoint the STR Responsible Officer so that he/she may examine the reports of suspicious transactions received and may send them to the FIU (without the name of the reporting person) if they are deemed grounded based on the elements available;
- identify the subjects (operators, managers of branches and central offices) who, within the scope of customer relation management, are bound to report, without delay, the transactions suspected of money laundering and terrorism financing to the STR Responsible Officer;
- identify a "Group STR Responsible Officer" as recipient of the information concerning the transactions reported by the Group foreign companies to their local Authorities, or the transactions filed by the same, in order to further analyse both the transactions reported as well as those filed, and evaluate them from a Group viewpoint²⁵;
- entrust the "Anti-Money Laundering Function" with the responsibility of assuring information flows for suspicious transaction reports, so that these may be addressed to the attention of the strategic function and supervisory function bodies of the Parent Company, of the Banks or of the Group Companies.

4.9 Compliance measures on counter terrorism, freezing of funds and economic resources, and on countering the proliferation of mass destruction weapons

In order to comply with the reference legislation concerning fund freezing, the Parent company establishes that the following protection measures be observed:

- financial services must not be provided to private individuals and legal persons included in the list of persons that commit, attempt to commit, take part in, or facilitate acts of terrorism;
- rule out altogether the possibility of placing, either directly or indirectly, funds or economic resources at the disposal of persons subject to fund-freezing measures or of allocating them for their benefit, thus preventing the person, group or entity from obtaining funds, assets or services;

²³ Document transmission must be performed, for the Group Banks, through the IT application provided; as regards non-banking companies, document transmission shall be made by means of a specific method that shall be defined in agreement with the Anti-money Laundering Department of the Parent Company (e.g., a the Certified Electronic Mail box provided).

²⁴ As regards non-banking companies of the Group under Italian law and foreign Companies, the aforementioned obligation shall be complied with only if contemplated, respectively, by primary and secondary applicable legislation as well as by local legislation.

²⁵ The Foreign Companies shall promptly send, via Certified Electronic Mail (PEC) to the Group Representative, the documentation pertaining to the transactions reported to the competent local authorities as well as that pertaining to the transactions filed.

- adopt suitable protection measures aimed at preventing involvement in development programs for the proliferation of weapons of mass destruction;
- in order to counter terrorist and international money laundering events, as well as the proliferation of mass destruction weapons, envisage specific supervisory procedures to verify that the legislation applicable to transactions involving assets classified as “dual use” assets are observed;
- refrain from taking part, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the fund-freezing measures;
- prevent frozen funds from being transferred, bank-ordered or used. In any case, freezing shall be without prejudice to the effects of any seizure or confiscation measures adopted within the scope of criminal or administrative proceedings;
- envisage procedures suitable to detect transactions or names of subjects that are potentially connected with the scope of the freezing obligations dealt with;
- notify the Financial Intelligence Unit and the Special Currency Police Unit of Guardia di Finanza (Italian tax police) of any freezing measures taken in compliance with the provisions of applicable national legislation²⁶ and, to this end, envisage procedures suitable to assure that the STR Responsible Officer promptly receives the information notice regarding the identification of potential transactions subject to the obligations herein.

4.10 Limits on the use of cash and bearer securities

In order to comply with the reference legislation concerning reporting of suspicious transactions, the Parent company establishes that the following protection measures be observed:

- inform the Ministry of Economy and Finance, within thirty days, of any infringement of the provisions pursuant to art. 49 of Italian Leg. Decree 231/07 of which knowledge has been gained²⁷, in detail:
 - the prohibition to transfer cash or bearer bankbooks or bearer securities in Euro or foreign currency²⁸, for any reason whatsoever between different persons, when the overall value being transferred exceeds or is equal to the threshold set by the legislation²⁹;
 - the obligation to indicate the name or company name of the beneficial owner and affix the non-transferability clause on the bank cheques issued for amounts above or equal to the threshold set by legislation³⁰;
 - the obligation to indicate the name or the company name of the beneficiary and to report the non-transferability clause on banker’s orders. In the event of banker’s orders below the threshold set by legislation,³¹ the non-transferability clause may be omitted upon written request by the customer and payment of the tax (stamp duty) prescribed by law;
 - the obligation to endorse bank cheques issued to the order of the drawer solely for collection at a Bank or at Poste Italiane S.p.A.;
 - the prohibition to transfer bearer savings bankbooks;
 - the obligation to extinguish bearer passbooks by the date established by Law (31 December 2018);

²⁶ Italian Legislative Decree no. 109 of 22 June 2007.

²⁷ In the event of infringements regarding cheques, banker’s orders, bearer passbooks or similar securities, notification must be made both by the Bank accepting them for their deposit and by the Bank that extinguishes them, unless there is the certainty that this has already been performed by the other obligor.

²⁸ Transfer shall be prohibited even when carried out with payments below the threshold, which appear to be artificially fractioned. However, the transfer may be carried out through banks, electronic money institutions and payment institutions (when these provide payment services other than those under art. 1, paragraph 1, lett. b), number 6), of Italian Leg. Decree No. 11 of 27 January 2010) and Poste Italiane S.P.A.

²⁹ On the date of entry into force of the Policy, the threshold is EUR 3,000 (this threshold was introduced by Law no. 208 of 28 December 2015).

³⁰ On the date of entry into force of the Policy the threshold is EUR 1,000 (this threshold has been introduced by Italian Law Decree no. 201 of 6 December 2011, converted with amendments by Italian Law no. 214 of 22 December 2011).

³¹ On the date of entry into force of the Policy the threshold is EUR 1,000 (this threshold has been introduced by Italian Law Decree no. 201 of 6 December 2011, converted with amendments by Italian Law no. 214 of 22 December 2011).

- observe the threshold set by legislation³² for the money remittance service pursuant to art. 1, par. 1, lett. b), no. 6) of Italian Legislative Decree 11/2010 (so called “money transfer”);
- issue bank cheque forms already provided with the non-transferability clause, subject to the possibility for the customer to request issuance of securities not bearing the said clause against payment of the relative taxation (stamp duties);
- collect cheques issued to the order of the drawer only if endorsed to the bank;
- issue banker's orders indicating the name or the company name of the beneficiary and the non-transferability clause, subject to the abovementioned exception concerning amounts below the threshold set by law;
- observe the obligation to issue savings bankbooks solely in the name of the bearer³³;
- comply with the prohibition to open - in whatever form - accounts or savings bankbooks in anonymous form or with fictitious names.

4.11 Protection measures for distribution networks and mediators

In order to comply with the reference legislation, the Parent company establishes that the following protection measures be observed in relation to the relative scope of application:

- define suitable organisation and IT procedures in order to ensure observance of the provisions on countering money laundering and terrorism financing;
- within the scope of "collaboration agreements" stipulated with financial agents and other external subjects connected with the Group Companies by means of contractual obligations designed to provide off-site products and services - define the rules of conduct aimed at complying with the reference legislation and therefore at countering money laundering and terrorism financing. Such rules shall be observed by the above subjects when performing activities on behalf of the Group, among which, with special reference to financial agents, when providing payment services or when issuing/distributing electronic money, the obligation to perform customer due diligence also in the event of occasional transactions involving amounts below 15,000 EUR;
- provide that the abovementioned subjects promptly notify the reference Company of the Group of all relevant circumstances and information for the purpose of allowing the latter to evaluate appropriate reporting of suspicious transactions;
- provide the subjects concerned with the operational instruments and procedures that may support them in meeting the obligations envisaged for anti-money laundering purposes when performing transactions;
- provide for the interruption of all relationships with financial agents and other subjects connected with the Group Companies by contractual obligations for the provision of off-site products, should they have committed, as ascertained, anti-money laundering/counter-terrorism breaches;
- define specific training programs for the subjects in question, so that they may be suitably knowledgeable with reference legislation and with the connected responsibilities, and so that they may use the instruments and procedures designed to support them in performing their obligations;
- continually monitor observance, by the sales network, of the rules of conduct within the scope of anti-money laundering/counter-terrorism as contractually laid down. In particular, it shall be verified that the financial agents appointed promptly³⁴ notify the Group Companies of the data and information provided by Art. 31 of Italian Leg. Decree 231/07;
- perform, at regular intervals, inspections at the operations centres of the persons in charge of the sales network;

³² At the date of Policy enforcement, the amount threshold for money remittances is 1,000 EUR.

³³ Pursuant to the provisions of Italian Leg. Decree 231/07, art. 49, all bearer savings bankbooks have been extinguished within 31st December 2018.

- verify how effectively collaborators apply the obligations of articles 24 and 25 of Italian Leg. Decree 231/2007 – “Enhanced customer due diligence”, in relation to which the Group Company provides its support.

In order to apply the above mentioned guidelines:

- the Italian Banks and non-banking companies of the Group that, for the off-site provision of their products, use networks of agents performing financial activities or other subjects linked to the same companies by contractual relationships, shall:
 - o draw up "collaboration agreements" based on those defined by the Parent Company;
 - o adopt training programs consistently with the training objectives laid down by the Parent Company;
 - o collaborate in performing the verification and monitoring activities conducted by the Parent Company;
- foreign Companies that, for the off-site provision of their products, use networks of agents performing financial activities or other subjects, shall:
 - o draw up "collaboration agreements" based on those defined by the Parent Company and taking into account applicable local legislation, as well as the operational and business specifications that characterise them;
 - o prepare training programs on the basis of those defined by the Parent Company and taking into account applicable local legislation, as well as the operational and business specifications that characterise them;
 - o collaborate in performing the verification and monitoring activities conducted by the Parent Company.

4.12 Protection measures regarding the reporting systems for internal violations (so called Whistleblowing)

In order to comply with the reference legislation, the Parent company establishes that the following protection measures be observed in relation to the relative scope of application:

- adopt specific procedures so that employees may report, internally, potential or actual violations of the provisions laid down to prevent money laundering and terrorism financing. Such procedures shall be capable of protecting the privacy of the subjects involved and or the reporting party.

5 Roles and Responsibilities of the Parent Company

5.1 Board of Directors

- defines, approves and periodically reviews the strategic guidelines and risk management policies connected with money laundering and terrorism financing for BPER Banca and for the Group; in compliance with a risk-based approach, such policies shall be suited to the extent and type of risk the business activity is actually exposed to. In this regard, also the results of the risk self-assessment practices - implemented by the Bank - in conformity with the indications received by the Supervisory Authority - shall be taken into account³⁵;
- approves the guidelines of the internal control system at an organic and coordinated Group level, designed to promptly detect and manage the risks of money laundering and terrorism financing, and assures its effectiveness over time;

³⁵ See Provisions of the Bank of Italy of 26 March 2019 “concerning organisation, procedures and internal controls” on anti-money laundering, Part Seven.

- defines and approves the risk objectives and the tolerance threshold;
- evaluates the adequacy of the overall management of the risk of money laundering and terrorism financing implemented by the Group;
- approves appointment of the "Anti-Money Laundering Function", to provide compliance with anti-money laundering and counter-terrorism legislation. Such function has an independent nature and plays a centralised role at the Parent Company for managing second-level controls on the risk of money laundering and terrorism financing. The Board identifies its tasks and responsibilities, as well as the coordination and collaboration methods with other corporate control functions;
- approves appointment of the Chief Anti-Money Laundering Officer (CAMLO), of the STR Responsible Officer for reporting suspicious transactions, and of the Group Representative, and approves their subsequent revocation, if any, after hearing the Board of Statutory Auditors;
- assures, on an ongoing basis, that the responsibilities and tasks regarding anti-money laundering and countering terrorist financing are allocated within the Group in a clear and appropriate manner, at the same time assuring that the operating and control functions are distinct and that such functions are provided with qualitatively and quantitatively appropriate resources;
- ensures that a suitable, complete and prompt system of information flows to the corporate bodies is in place, always assuring protection of the confidentiality of the subjects that have taken part in reporting procedure for a suspicious transaction;
- defines and approves the formalised procedures for coordination, information sharing and connection between the Parent Company and the Group Companies as regards the management of money laundering risk.
- examines and approves, at least every year, the reports on the activity performed and on the inspections carried out by the Anti-Money Laundering Function. The Board also approves the document on the results of the self-assessment procedure applicable to money laundering risks³⁶;
- assures that the deficiencies and anomalies found as a result of the inspections performed on different levels are promptly brought to their knowledge, and promotes the adoption of suitable corrective measures, evaluating their efficacy;
- with this Policy, the Board approves the principles for managing the relationships with "high-risk" customers connected with the risk of money laundering and terrorism financing, and it identifies the protection measures to adopt in order to limit the risks linked to transactions with the highest risk third countries.

5.2 Board of Statutory Auditors

- audits the Internal Control System set up to monitor the risk of money laundering and terrorism financing;
- supervises that anti-money laundering legislation is observed and that the System adopted is complete, appropriate and functional.
- evaluates the appropriateness of the existing procedures applicable to customer due diligence, to information storage and to the reporting of suspicious transactions;
- analyses the reasons for the deficiencies, anomalies and irregularities found and promotes the adoption of appropriate corrective measures.

The Board of Statutory Auditors expresses its opinion on the decisions concerning the appointment of the Chief Anti-Money Laundering Officer (CAMLO) and on the reporting of suspicious transactions, as well as on the definition of the overall system for managing and controlling the risk of money laundering and terrorism financing.

As regards the relationships with the Supervisory Authorities, the members of the Board of Statutory Auditors shall promptly inform the Bank of Italy of all facts or actions that come to their knowledge during performance of their functions and that may constitute serious, repeated or systematic violation of applicable laws provisions and of the related enforcement provisions.

³⁶ See previous note.

5.3 Chief Executive Officer (CEO)³⁷

- provides for the implementation of the strategic guidelines and risk management policies on money laundering and terrorism financing, as defined by the Board of Directors, and he/she is responsible for taking the necessary measures to assure the effectiveness of the organization and monitoring systems on this matter;
- takes care of the implementation of an internal monitoring system aimed at promptly detecting and managing the money laundering risk, observing the guidelines laid down by the Board of Directors, and ensures its efficacy over time. In this regard, he/she also takes into account evidence resulting from risk self-assessment procedures carried out by the Bank, consistently with the instructions received by the Supervisory Authority³⁸;
- puts in place the initiatives and actions required to assure that the architecture of control functions is consistent with the complexity of the activities performed, the dimension of the internal organization, the type of products and services offered and the extent of the risk that may be linked to the customer characteristics, thus guaranteeing the overall reliability of the Internal Control System over time;
- establishes the coaching and training programmes for employees and collaborators on the obligations arising from the guidelines on anti-money laundering and financing of international terrorism;
- establishes the suitable instruments for allowing ongoing monitoring of the activities carried out by employees in order to detect any anomalies arising in the conduct, information flows with contact persons and the company departments, and in the relationships with customers;
- assures that the operating procedures and information systems are appropriate in order to comply with anti-money laundering and counter-terrorism obligations;
- provides for the organisational and procedural changes necessary to assure adequate protection measures for the offences of money laundering and terrorism financing;
- defines the actions and procedures to assure prompt fulfilment of the obligation to report to the Authorities, as laid down by the legislation on money laundering and the financing of terrorism;
- as regards reporting suspicious transactions, he/she defines and takes care of the implementation of a procedure capable of assuring reference certainty, homogeneous behaviours, generalised application to the entire organisation, complete use of the relevant information and traceability of the assessment process. The Chief Executive Officer (CEO) also adopts measures aimed at guaranteeing strict confidentiality on the identity of the persons that have taken part in the reporting procedure as well as the instruments (including electronic instruments) used for detecting the anomalous transactions;
- defines and takes care of the implementation of information procedures aimed at assuring that the employees, at all organizational levels, and the bodies with supervisory functions are aware of the risk factors and of the company protection measures on anti-money laundering and countering of terrorism connected with their tasks and related responsibilities;
- with this Policy, he/she defines the management procedures for the relationships with the customers identified as "high risk" subjects in connection with money laundering/terrorism financing, consistently with the principles laid down by the Board of Directors.

5.4 General Manager

The General Manager, or other holder of management and administrative functions, or person entrusted by the same³⁹:

- assesses and authorises:

³⁷ The Chief Executive Officer (CEO) is the Director who performs the functions envisaged by the Provisions issued by the Bank of Italy on 26/3/19 "as regards the organisation, procedures and controls" on anti-money laundering.

³⁸ See Provisions of the Bank of Italy of 26 March 2019 "concerning organisation, procedures and internal controls" on anti-money laundering, Part Seven.

³⁹ Or, however, subjects performing an equivalent function.

- opening of current accounts with correspondent bodies in third Countries for the Group Companies under Italian and foreign Law;
- establishment/prosecution of an ongoing relationship, or performance of occasional transactions with "politically exposed persons" (so called "PPE") for the Parent Company;
- receives information on the authorisations provided by the Banks and by the Group Companies under Italian Law as regards the establishment/prosecution of an ongoing relationship, or performance of occasional transactions with "politically exposed persons" (so called "PPE").

5.5 STR (Suspicious Transactions Reports) Responsible Officer

- evaluates the reports on suspicious transactions of money laundering or terrorism financing received or that came otherwise to his/her knowledge within the scope of his/her activity, and h/she notifies such transactions, if deemed grounded, to the FIU, or he/she dismisses them;
- manages the relationships with the FIU, promptly responding to any requests for further investigation submitted by the same;
- assures promptness and confidentiality of the suspicious transaction reporting process by the Bank;
- keeps evidence of the assessments made, also if a report is not sent to the FIU;
- ensures that the policies and procedures for detecting and reporting suspicious transactions are observed, promptly notifying the Bank corporate bodies of any issues found;
- when requested, he/she submits a report on the detection, analysis and reporting of suspicious transactions to the FIU, to the Bank corporate Bodies.
- ensures observance of the procedures for identifying and reporting suspicious transactions;
- has free access, directly or through the organisation facilities he/she coordinates, to the information flows and archives (both on paper and electronic means), as well as to all information that may be relevant for performance of his/her tasks.

5.6 Group STR Responsible Officer

- analyses and evaluates, from a Group viewpoint, the reports filed and the transactions reported by the Italian Companies to the FIU, as well as those reported by the Group foreign Companies to their competent local Authorities;
- at least every year, he/she submits - to the corporate Bodies of the Parent Company - a report on the identification, analysis and reporting of suspicious transactions from a Group viewpoint;
- has free access, directly or through the organisation facilities he/she coordinates, to the information flows and to all databases (both on paper and electronic means) of the Group, as well as to all information that may be relevant for performance of his/her tasks.